VECTRA
SECURITY THAT THINKS.®

CASE STUDY

Network detection and response to business email compromise attacks

Overview

Vectra® recently helped identify and stop a phishing-free BEC scam at an EU-based manufacturing company that was running Cognito Detect for Office 365 on its Cognito® Network Detection and Response (NDR) platform.

The attack

The attackers targeted users in the finance department, most likely identified as such via LinkedIn reconnaissance. Rather than leverage a phishing attack – or maybe because phishing attempts hadn't worked – the attackers instead gained direct access to two accounts using a low-and-slow brute-sweep attack.

The attack ran over an extended time period to avoid lockout protection and against legacy protocols to bypass multifactor authentication (MFA). With Office 365 credentials in hand, the attackers then setup multiple mail rules in each compromised account:

1. Monetize the compromise: Forward all emails with special considerations for *DocuSign* or *invoices*.
2. Ensure long-term persistence: Delete all emails related to *security* and *passwords*.

Other than creating these mail rules, the attacker progressed no further. Cognito Detect for Office 365 identified the account takeovers and the security team promptly deleted the rules and reset passwords before any emails were forwarded.

$26B **Fraud originating from business email compromise (BEC) is a $26 billion problem for businesses, according to the FBI.**

Although the most common BEC is associated with phishing, smart cyberattackers are now bypassing phishing altogether.

Account takeover in Microsoft 365 has become the largest threat vector in the cloud.

What the Cognito platform saw

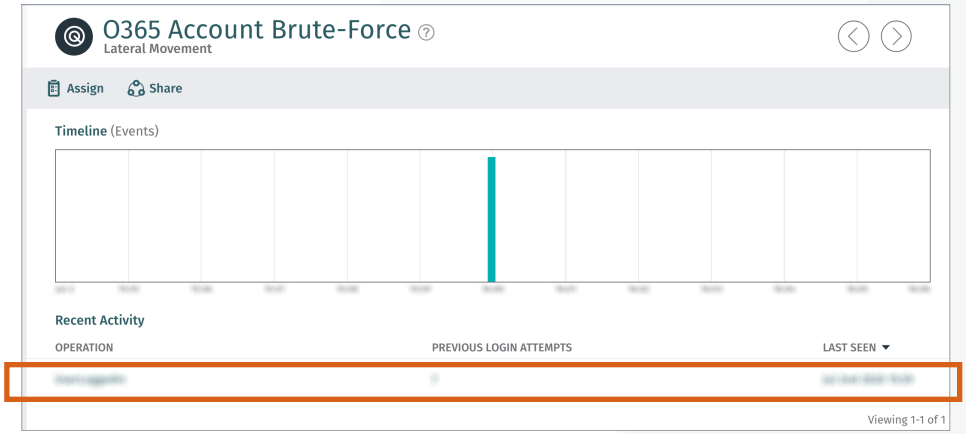
All the steps in this attack were made visible by Cognito Detect for Office 365, spanning the initial account takeover to the creation of email rules.

Looking at the Cognito platform console, the attacker's successful brute sweep was clearly identified as well as the suspect nature of the successful sign-on events for the two accounts involved in the incident.

Interestingly, the IP addresses the attackers used to sign in appeared to be within the same geolocation as the firm's legitimate users. While the location information may have been normal, the machine learning algorithms in Cognito Detect look at all aspects of the sign-on events – including the sign-in method and user agent – to identify anomalous logins and ensure that attackers cannot avoid detection.

Because Cognito Detect for Office 365 provides full detection capabilities beyond initial access, the attackers' actions related to evasive email-rule creation and email forwarding also triggered alerts.

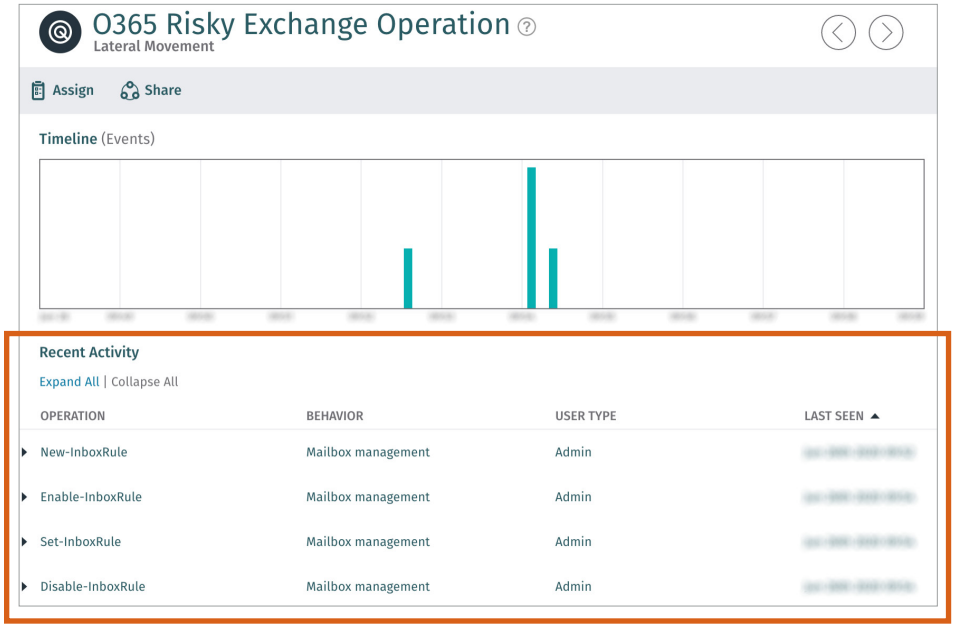
The actions related to the rule creation were clearly highlighted by the Cognito Detect *risky exchange operation* detection, which reported multiple anomalous user operations related to creating and modifying email rules.

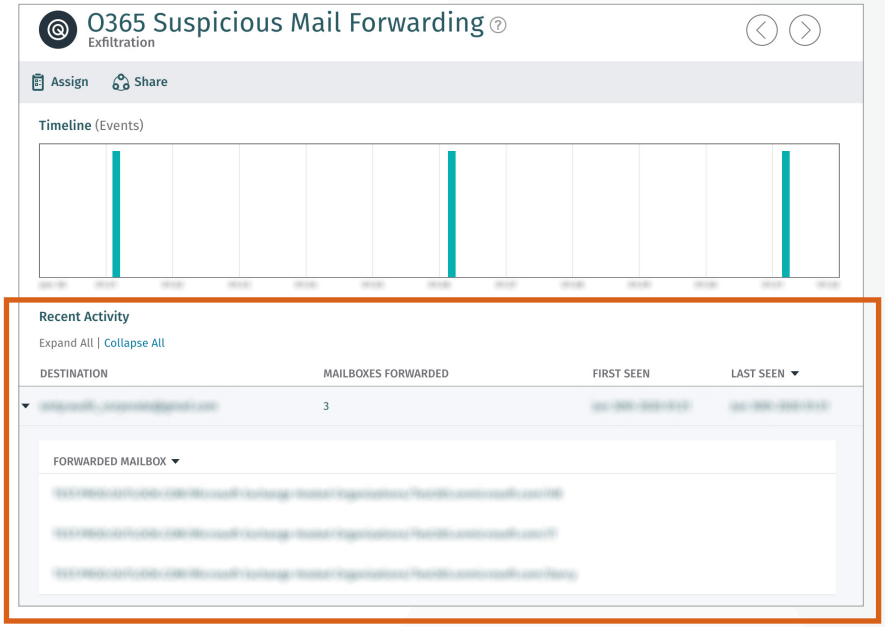


While the location information may have been normal, the machine learning algorithms in Cognito Detect look at all aspects of the sign-on events – including the sign-in method and user agent – to identify anomalous logins and ensure that attackers cannot avoid detection.

Investigating the details of these operations reveals that one of the rules would have hidden any emails from IT that could have resulted in a password reset for the account and another rule that would have forwarded messages related to *DocuSign* and *invoice* to the attacker's Gmail account.

Regarding the collection of specific emails, the attackers attempted to have a more complete record of the compromised account emails by forwarding the entire mailbox to a second Gmail address. This anomalous action was quickly detected using the Cognito Detect *suspicious mail forwarding* detection.





The combination of behaviors observed in the compromised account resulted in Cognito Detect prioritizing the accounts and allowing the security team to respond promptly before any emails were forwarded. The account's password was reset and the external IP address was blocked.

For more information about the Vectra NDR platform and Cognito Detect for O365, please contact a service representative at sales-inquiries@vectra.ai.

Email info@vectra.ai vectra.ai